

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**

THIS PAGE BLANK (USPTO)

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets

(11)

EP 0 875 871 A2

(11)

(12)

EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
04.11.1998 Patentblatt 1998/45

(51) Int. Cl.⁶: G07F 19/00, G07F 7/10,
G07C 9/00

(21) Anmeldenummer: 98100688.5

(22) Anmeldetag: 16.01.1998

(84) Benannte Vertragsstaaten:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC
NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: 29.04.1997 DE 19718103

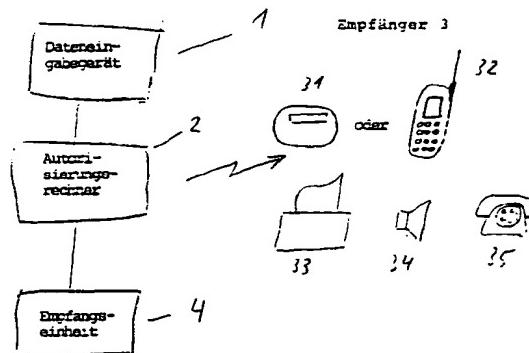
(71) Anmelder: Schmitz, Kim
80539 München (DE)

(72) Erfinder: Schmitz, Kim
80539 München (DE)

(74) Vertreter:
Freiherr von Gravenreuth, Günter, Dipl.-Ing. (FH)
Schwanthalerstrasse 3
80336 München (DE)

(54) Verfahren zur Autorisierung in Datenübertragungssystemen

(57) Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Autorisierung in Datenübertragungssystemen unter Verwendung einer Transaktionsnummer (TAN) oder eines vergleichbaren Paßworts, wobei der Benutzer in einem 1. Schritt über ein Dateneingabegerät seine Identifizierung und/oder eine Identifizierungs-Kennung des Dateneingabegeräts zusammen mit der Aufforderung zur Generierung oder zur Auswahl einer TAN oder ein vergleichbares Paßwort aus einer Datei an einen Autorisierungsrechner sendet, in einem 2. Schritt der Autorisierungsrechner die TAN oder das vergleichbare Paßwort generiert oder aus einer Datei auswählt, in einem 3. Schritt der Autorisierungsrechner die TAN oder das vergleichbares Paßwort über einen anderen Übertragungsweg als in Schritt 1 an einen Empfänger (z. B. Handy oder Pager) sendet, in einem 4. Schritt der Benutzer diese TAN oder das vergleichbare Paßwort von dem Empfänger übernimmt und in das Dateneingabegerät eingibt, in einem 5. Schritt diese TAN oder das vergleichbare Paßwort wieder an den Autorisierungsrechner übermittelt wird, in einem 6. Schritt der Autorisierungsrechner die Gültigkeit der TAN oder des vergleichbaren Paßworts prüft, um dann in einem 7. Schritt einen Verbindungsauflauf zwischen dem Dateneingabegerät und einer Empfangseinheit herzustellen oder freizuschalten.



Beschreibung

Die Erfindung betrifft ein Verfahren zur Autorisierung in Datenübertragungssystemen.

Es ist bekannt, daß beim Telebanking der Benutzer neben seinem permanenten Passwort (PIN) für jede einzelne Transaktion noch zusätzlich eine Transaktionsnummer (TAN) benötigt. Derartige TAN's werden in größeren Blöcken dem Benutzer mit der Post übermittelt. Es besteht daher das Risiko, daß Dritte von derartigen TAN's Kenntnis erlangen und in Verbindung mit dem Passwort einen Mißbrauch vornehmen können. Das Risiko wird dadurch erhöht, daß derartige TAN's faktisch eine zeitlich unbegrenzte Gültigkeit besitzen.

Bekannt sind ferner Call-Back-Systeme, bei denen das angerufene System sich durch einen Rückruf bei einer im Regelfall gespeicherten Nummer vergewissert, daß das anrufende System autorisiert ist und nicht ein fremdes System sich für ein berechtigtes System ausgibt. Der Nachteil der Call-Back-Systeme besteht darin, daß ein unbefugter Benutzer, welcher sich aus einer beliebigen Quelle einen funktionalen Zugang zu dem berechtigten anrufenden System verschafft hat, unter dieser rechtswidrig erlangten Berechtigung problemlos arbeiten kann, da das Call-Back-System nur überprüft, ob es von einem grundsätzlich berechtigten System aus angerufen wurde.

Der Erfindung liegt die Aufgabe zugrunde ein Verfahren zur Autorisierung in der Datenübertragung zu schaffen, in dem die Sicherheit erhöht wird. Dieses Verfahren wird erfindungsgemäß durch den kennzeichnenden Teil des Anspruchs 1) gelöst.

Drahtlose Telekommunikationsgeräte wie beispielsweise Handys oder Pager besitzen oft die Möglichkeit, kurze (alpha-)numerische Nachrichten (z. B. der Short Message Service = SMS-Dienst) zu empfangen und auf ihrem Display anzuzeigen. Die vorliegende Erfindung nutzt diese Möglichkeit, um eine TAN oder ein vergleichbares Passwort zu übermitteln.

Nach der vorliegenden Erfindung übermittelt der Benutzer über ein Dateneingabegerät seine Identifizierung (User-ID, Passwort o. ä.) und/oder eine Identifizierungs-Kennung des Dateneingabegeräts zusammen mit einer Aufforderung zur Generierung einer TAN (oder eines vergleichbaren Passworts) an einen Rechner, welcher den Autorisierungsvorgang übernimmt und nachfolgend kurz Autorisierungsrechner genannt wird. In diesem Autorisierungsrechner wird durch einen Zufallsgenerator eine alphanumerische oder nur numerische TAN (oder eine vergleichbare Passwort) errechnet oder einer Datei entnommen. Dann wird von dem Autorisierungsrechner parallel zur bestehenden Verbindung mit dem Dateneingabegerät, über einen anderen Übertragungsweg diese TAN (oder ein vergleichbares Passwort) an einen Empfänger übermittelt. Dieser Empfänger kann beispielsweise

- a) ein Funkempfänger mit einem Display oder

Monitor wie z. B. ein Handy, ein Pager (z. B. einen Cityruf-Empfänger),

- b) eine speziell gestaltete Empfangskarte innerhalb des Dateneingabegerätes, welche über Funk oder eine feste Verdrahtung angesprochen wird,
- c) eine Mailbox,
- d) ein Telefax- oder
- d) ein Sprachausgabegerät wie ein fest installierter Lautsprecher oder ein (Sprach-)Telefon

sein. Hierzu verfügt der Autorisierungsrechner über die erforderliche(n) Telefon-, Funkruf- oder Faxnummern, E-Mail- oder Netzadresse(n). Die diesbezüglichen Daten sind üblicherweise im Autorisierungsrechner gespeichert. Es ist jedoch möglich, daß der Autorisierungsrechner seinerseits sich diese Daten aus einer Datenbank holt, welche sich auf einem anderen Rechner befindet. Insoweit kann auch der Autorisierungsrechner unter Verwendung des erfindungsgemäß Verfahrens von sich aus einen Zugriff auf diesen anderen Rechner tätigen.

Der berechtigte Benutzer kann die ihm so übermittelte TAN (oder das vergleichbare Passwort) manuell in sein Dateneingabegerät eingeben und wieder an den Autorisierungsrechner versenden. Bei automatisierten Verfahren erfolgt erfindungsgemäß eine automatische Übertragung der TAN (oder des vergleichbaren Passworts). Der Autorisierungsrechner überprüft nunmehr die Übereinstimmung zwischen allen (von ihm vergebenen) gültigen TAN's (oder vergleichbaren Passwörtern) und ermöglicht nach dieser Autorisierungsprüfung eine Freigabe des Datenflusses zwischen dem Dateneingabegerät und einer Empfangseinheit.

Bei der TAN (oder dem vergleichbaren Passwort) kann es sich um eine nur einmal verwendbare TAN handeln. Es sind jedoch auch andere Begrenzungen wie die Benutzerzeit und/oder die Zahl oder Größe der übertragenen Dateien für die Gültigkeit der TAN (oder des vergleichbaren Passworts) denkbar.

Nach dem in vorgenannter Weise autorisierten Verbindungsauflauf können nunmehr Daten von dem Dateneingabegerät an die Empfangseinheit (oder umgekehrt; Voll duplex) übermittelt werden.

Es liegt auf der Hand, daß zur zusätzlichen Sicherheit diese Daten auch verschlüsselt werden können.

Sowohl das Dateneingabegerät, als auch der Autorisierungsrechner und die Empfangseinheit können normale (Personal-)Computer sein. Die Erfindung arbeitet plattformunabhängig, d. h. sie ist unabhängig von Prozessortypen, Betriebssystemen und/oder Steuerelektroniken (z. B. der Empfangseinheit) und/oder Input/Output-Einheiten (z. B. des Dateneingabegeräts und der Empfangseinheit).

Die Sicherheit dieses Systems liegt darin, daß nur bei einer Autorisierung der Geräte eine Datenübertragung von dem Dateneingabegerät an die Empfangseinheit durch den Autorisierungsrechner freigeschaltet wird. Dies wird durch den Einsatz getrennter Übertra-

gungswege zwischen dem Dateingabegerät und dem Autorisierungsrechner einseits und dem Autorisierungsrechner und der TAN-Übertragung andererseits, erreicht. Insoweit unterscheidet sich die Erfindung von Call-Back-Systemen bei denen nur eine Überprüfung zwischen dem Dateneingabegerät und dem Autorisierungsrechner erfolgt.

Das erfindungsgemäße Verfahren ermöglicht verschiedene Sicherheitsstufen.

Auf dem niedrigsten erfindungsgemäßen Sicherheitsniveau wird in dem Dateneingabegerät als Empfänger ein Funkempfänger beispielsweise in Form einer Steckkarte eingebaut, so daß nur mit diesem konkreten Gerät eine Datenübertragung an die Empfangseinheit möglich ist. Zur Erhöhung dieser Sicherheit kann vorgesehen werden, daß dieser Funkempfänger nur mit einem Benutzer-Identifizierungselement, beispielsweise einer Magnet- oder Chipkarte betrieben werden kann. Das Benutzer-Identifizierungselement kann auch mit grafischen Methoden wie Überprüfung eines Fingerabdruckes oder Bildidentifizierung des Benutzers arbeiten.

Die weitere erfindungsgemäße Sicherheitsstufe besteht darin, daß der Autorisierungsrechner die TAN (oder das vergleichbare Paßwort) an einen Pager oder ein vergleichbares Gerät übermittelt. In diesem Fall erfolgt eine Autorisierung nur dann, wenn das Dateneingabegerät und der Pager im Zugriff derselben Person sind. Nur dann ist es möglich, daß die auf dem Display des Pagers angezeigte TAN (oder ein vergleichbares Paßwort) in das Dateneingabegerät eingegeben und von dort wieder an den Autorisierungsrechner übermittelt wird.

Auf einen Pager übermittelte Daten können bekannterweise jedoch abgehört werden. Eine weitere erfindungsgemäße Sicherheitsstufe kann in der Weise erzielt werden, daß im Autorisierungsrechner und im Pager übereinstimmende Verschlüsselungs-Module im Einsatz sind.

Anstelle des Pagers oder Handys kann auch in erfindungsgemäßer Weise ein anderes Empfangsgerät vorgesehen sein. Dies kann eine Mailbox, ein Telefax oder ein Sprachausgabegerät sein. Als Sprachausgabegerät sind erfindungsgemäß fest installierte Lautsprecher oder die Übertragung der Sprache auf einen definierten Telefonanschluß möglich. Bei den Sprachausgabengeräten erfolgt eine sprachliche Ausgabe der TAN (oder des vergleichbaren Paßworts).

Es liegt auf der Hand, daß auch die Übertragung auf derartige Empfangsgeräte verschlüsselt werden kann.

Wenn anstelle eines Pagers ein Handy, insbesondere ein GSM-Handy, im Einsatz ist, dann kann man infolge der Verschlüsselung der diesbezüglichen Übertragungstechnik erfindungsgemäß auf weitere Verschlüsselungsmechanismen verzichten. In diesem Fall erfolgt die Anzeige der TAN (oder des vergleichbaren Paßworts) auf dem Display des Handys.

Eine weitere erfindungsgemäße Sicherheitsstufe kann dadurch erreicht werden, daß zwischen dem Dateneingabegerät und dem Autorisierungsrechner eine Verbindung nur dann aufgebaut wird, wenn über das Dateneingabegerät ein entsprechendes Passwort übermittelt wird. Dieses Passwort kann erfindungsgemäß eine wesentlich längere zeitliche Gültigkeit besitzen als die TAN.

Eine weitere erfindungsgemäße Sicherheitsstufe kann dadurch erreicht werden, daß bereits zur Benutzung des Dateneingabegerätes ebenfalls ein Passwort erforderlich ist.

Es liegt auf der Hand, daß eine Kombination der vorgenannten Sicherheitsstufen möglich ist.

Die Erfindung ist universell im Bereich der Datenübertragungssysteme einsetzbar. Dies gilt beispielsweise auch für das Internet und Intra-Netze, Local-Area-Networks (LAN), Wide-Area-Networks (WAN) etc..

Das fragliche System ist auch außerhalb der klassischen EDV beispielsweise bei physischen Zugangskontrollen einsetzbar. Der Benutzer gibt hierzu beispielsweise auf einer in Nähe angebrachten Tastatur (= Dateneingabegerät) sein persönliches Passwort ein. Der Autorisierungsrechner prüft dieses Passwort, ggf. auch in Verbindung mit der Zugangsberechtigung zu dem konkreten - zur konkreten Zeit - Raum. Wenn das betreffende Passwort (noch) gültig ist, übermittelt der Autorisierungsrechner an ein

Handy oder ein für das spezielle Türschließ-System konzipierte, funktional mit einem Pager vergleichbares Gerät, die TAN (oder das vergleichbare Paßwort). Anschließend wird diese TAN (oder das vergleichbare Paßwort) vom Benutzer manuell über die in Nähe angebrachte Tastatur eingegeben und automatisch an den Autorisierungsrechner weitergeleitet. Nach erfolgreicher Überprüfung erfolgt vom Autorisierungsrechner ein Signal für die Freigabe des Türschließ-Mechanismus. Diese Freigabe kann ggf. zeitlich begrenzt sein.

Die Empfangseinheit kann in diesem Fall in technischer Hinsicht einfachster Natur sein, da sie nur das Signal für die Freigabe des Türschließ-Mechanismus so verarbeiten muß, daß die betreffende Elektro-Mechanik die Tür zum Öffnen freigibt.

So ist es möglich ein System aufzubauen, bei dem unterschiedliche Personen unterschiedliche Berechtigung zur Betretung verschiedener Räume haben.

Die konkreten Anwendungsfelder umfassen, z.B.:

- 50 - Rechenzentren
- Flughäfen
- Ministerien
- Zoll
- Grenzübergänge
- 55 - Sicherheitsbereiche
- Banken
- Tresore
- Garagen

- Parkhäuser
- Autos

Das gesamte System erhält seine Sicherheit aus der Kombination mehrerer unterschiedlicher Basisprinzipien und Faktoren:

(1) "what-you-have" (die nicht zu duplizierende (GSM)-Chipkarte), also ein physisches Unikat, das nicht verlustfrei weitergegeben werden kann.

(2) "what-you-know" (die PIN der GSM-Chipkarte sowie den eigenen Benutzernamen im Dateneingabegerät und/oder Authentifizierungsserver), also Know-How, das nicht unabsichtlich oder versehentlich weitergegeben werden kann

(3) DES-Verschlüsselung und kryptografische Authentifikation im GSM-Netz selbst, dadurch Resistenz gegen Abhör- und Manipulationsangriffe

Dadurch ist zur Kompromittierung des Systems die Kombination mindestens dreier - jeweils für sich schon sehr unwahrscheinlicher - Ereignisse von nötig:

- a) physischer Verlust der (Handy-)Chipkarte, des Pagers oder ein fremder Zugriff auf die Mailbox, das Telefax- oder Sprachausgabegerät,
- b) Herausgabe der PIN des Empfängers (z. B. von der Chipkarte oder des Handy) und
- c) Kenntnis der übermittelten TAN oder des vergleichbaren Paßwortes.

Ein versehentliches Zusammentreffen dieser Faktoren ist nahezu auszuschließen, zumal auch in diesem Fall der erfolgreiche Angriff auf das System die intime Kenntnis des Zugangsverfahrens und der Benutzer-ID voraussetzt, die bei einem Angriff im Normalfall nicht gegeben ist. Außerdem hat der Nutzer die Möglichkeit, seine Benutzer-ID bei Verlust seiner Chipkarte beim Authentifizierungsserver sofort zu sperren oder sperren zu lassen.

Ein weiterer Vorteil der Abstützung auf GSM besteht darin, daß der Benutzer während des Autorisierungsvorganges jederzeit erreichbar ist, also z.B. bei Zugangsproblemen oder Zweifeln an seiner Identität vom Systembetreuer direkt angerufen werden kann.

Diese Lösung hat den Vorteil, daß sie sehr sicher, kostengünstig und mit herkömmlicher, weit verbreiteter und sicherer Hardware realisierbar ist.

Eine weitere erfindungsgemäße Lösung besteht darin, daß Autorisierungsrechner und Empfangseinheit ein Gerät sind.

Weitere Vorteile und Anwendungsmöglichkeiten der Erfindung ergeben sich aus dem nachfolgend benannten Ausführungsbeispiel in Verbindung mit der Zeichnung.

Ein berechtigter Benutzer betätigt ein Dateneinga-

begerät 1). Hierüber sendet er die Aufforderung zur Generierung oder Auswahl und Rücksendung einer TAN (oder eines vergleichbaren Paßwortes) an einen Autorisierungsrechner 2). Der Autorisierungsrechner 2) generiert die TAN (oder ein vergleichbares Paßwort). Dem Autorisierungsrechner 2) ist die Rufnummer oder Datenadresse, z. B. die E-Mail- oder Netz-Adresse des Empfängers (3) des Benutzers des Dateneingabegerätes 1) bekannt. Er sendet an einen Empfänger 3) (nicht näher dargestellt) diese TAN (oder ein vergleichbares Paßwort). Der Empfänger 3) kann ein Pager 31) oder ein Handy 32) sein. Der Empfänger 3) kann jedoch auch die E-Mail-Adresse einer Mailbox (nicht dargestellt), ein Telefax-Gerät 33) oder ein Sprachausgabegerät sein. Das Sprachausgabegerät kann ein fest installierter Lautsprecher 34) oder ein Telefon 35) sein. Der Benutzer läßt diese TAN (oder ein vergleichbares Paßwort) vom Empfänger 3) ab oder hört sie von der Sprachausgabe und gibt sie manuell in das Dateneingabegerät 1) ein. Das Dateneingabegerät 1) übermittelt nunmehr die TAN (oder ein vergleichbares Paßwort) an den Autorisierungsrechner 2). Der Autorisierungsrechner 2) überprüft, ob diese TAN (oder das vergleichbare Paßwort) noch gültig ist. Zu diesem Zweck kann der Autorisierungsrechner so programmiert sein, daß die Gültigkeit der TAN (oder des vergleichbaren Paßworts) zwischen ihrer Versendung an den Empfänger 3) und ihre Übermittlung über das Dateneingabegerät 1) zeitlich begrenzt ist. Die zeitliche Begrenzung kann beispielsweise zwei Minuten betragen. Wenn die TAN (oder das vergleichbare Paßwort) gültig ist, dann stellt der Autorisierungsrechner 2) eine Verbindung zu einer Empfangseinheit 4) her. Nunmehr ist der Benutzer für die Dauer der Aufrechterhaltung dieser Verbindung in der Lage, Daten vom Dateneingabegerät 1) an die Empfangseinheit 4) zu übermitteln und/oder zu empfangen.

Es liegt auf der Hand, daß diese Daten zur weiteren Sicherung verschlüsselt werden können.

Denkbar ist ferner, daß nicht nur die TAN (oder das vergleichbare Paßwort) hinsichtlich ihrer Gültigkeit eine zeitliche Begrenzung hat, sondern daß auch die Dauer der Aufrechterhaltung der Verbindung zwischen dem Dateneingabegerät 1) und der Empfangseinheit 4) zeitlich begrenzt ist. Hierdurch kann vermieden werden, daß eine "Standleistung" zwischen dem Dateneingabegerät 1) und der Empfangseinheit 4) hergestellt wird, was wiederum eine Sicherheitslücke darstellen könnte.

Der Autorisierungsrechner 2) und die Empfangseinheit 4) können ein einziger Computer sein. In diesem Fall erfolgt ein erster Zugriff auf ein Datenverarbeitungsprogramm, welches den Autorisierungsvorgang (Generierung und Übermittlung der TAN) in vorgenannter Weise durchführt. In einem zweiten Schritt erfolgt dann die Datenübertragung.

Es können sogar das Dateneingabegerät (1), der Autorisierungsrechner (2) und die Empfangseinheit (4) ein einziger Computer sein. In diesem Fall erfolgt ein

erster Zugriff auf ein Datenverarbeitungsprogramm, welches den Autorisierungsvorgang (Generierung und Übermittlung der TAN an den Empfänger) in vorgenannter Weise durchführt. Erst nach der Autorisierung erhält der Benutzer einen vollen oder auf gewisse Bereiche beschränkten Rechnerzugang.

Bezugszeichenliste

Dateneingabegerät	1)
Autorisierungsrechner	2)
Empfänger	3)
Pager	31)
Handy	32)
Telefax-Gerät	33)
Lautsprecher	34)
Telefon	35)
Empfangseinheit	4)

Patentansprüche

1. Verfahren zur Autorisierung in Datenübertragungssystemen unter Verwendung einer Transaktionsnummer (TAN) oder eines vergleichbaren Paßworts, dadurch gekennzeichnet,
 - daß der Benutzer in einem 1. Schritt über ein Dateneingabegerät (1) seine Identifizierung und/oder eine Identifizierungs-Kennung des Dateneingabegeräts (1) zusammen mit der Aufforderung zur Generierung oder zur Auswahl einer TAN oder eines vergleichbaren Paßworts aus einer Datei an einen Autorisierungsrechner (2) sendet,
 - daß in einem 2. Schritt der Autorisierungsrechner (2) die TAN oder das vergleichbare Paßwort generiert oder aus einer Datei auswählt,
 - daß in einem 3. Schritt der Autorisierungsrechner (3) die TAN oder das vergleichbare Paßwort über einen anderen Übertragungsweg als in Schritt 1 an einen Empfänger (3) sendet,
 - daß in einem 4. Schritt der Benutzer diese TAN oder das vergleichbare Paßwort von dem Empfänger (3) übernimmt und in das Dateneingabegerät (1) eingibt,
 - daß in einem 5. Schritt diese TAN oder das vergleichbare Paßwort wieder an den Autorisierungsrechner (2) übermittelt wird,
 - daß in einem 6. Schritt der Autorisierungsrechner (2) die Gültigkeit der TAN oder des vergleichbaren Paßworts prüft, um dann
 - in einem 7. Schritt einen Verbindungsauflauf zwischen dem Dateneingabegerät (1) und einer Empfangseinheit (4) herzustellen oder freizuschalten.
2. Verfahren nach Anspruch 1), dadurch gekennzeichnet, daß es sich um eine nur einmal verwend-

bare TAN oder eine vergleichbares Paßwort handelt.

3. Verfahren nach einem oder mehreren der Ansprüche 1) bis 2), dadurch gekennzeichnet, daß die Gültigkeit der TAN oder des vergleichbaren Paßworts eine vordefinierte Benutzerzeit ist.
4. Verfahren nach einem oder mehreren der Ansprüche 1) bis 3), dadurch gekennzeichnet, daß die Gültigkeit der TAN oder des vergleichbaren Paßworts von einer vordefinierten Anzahl der übertragenen Dateien abhängig ist.
5. Verfahren nach einem oder mehreren der Ansprüche 1) bis 4), dadurch gekennzeichnet, daß die Gültigkeit der TAN oder des vergleichbaren Paßworts von einer vordefinierten Größe der übertragenen Dateien abhängig ist.
6. Verfahren nach einem oder mehreren der Ansprüche 1) bis 5), dadurch gekennzeichnet, daß der Zugriff auf das Dateneingabegerät (1) und/oder der Empfänger (3) und/oder die Empfangseinheit (4) durch ein Passwort geschützt ist.
7. Verfahren nach einem oder mehreren der Ansprüche 1) bis 6), dadurch gekennzeichnet, daß die von dem Dateneingabegerät (1) an die Empfangseinheit (4) oder umgekehrt übermittelten Daten verschlüsselt sind.
8. Verfahren nach einem oder mehreren der Ansprüche 1) bis 7), dadurch gekennzeichnet, daß die von dem Dateneingabegerät (1) an den Autorisierungsrechner (2) oder umgekehrt übermittelten Daten verschlüsselt sind.
9. Vorrichtung zur Ausführung des Verfahrens nach einem oder mehreren der Ansprüche 1) bis 8), dadurch gekennzeichnet, daß der Empfänger (3) ein Pager (31) ist.
10. Vorrichtung zur Ausführung des Verfahrens nach einem oder mehreren der Ansprüche 1) bis 8), dadurch gekennzeichnet, daß der Empfänger (3) ein Handy (32) ist.
11. Vorrichtung zur Ausführung des Verfahrens nach einem oder mehreren der Ansprüche 1) bis 8), dadurch gekennzeichnet, daß der Empfänger (3) ein Telefax (33) ist.
12. Vorrichtung zur Ausführung des Verfahrens nach einem oder mehreren der Ansprüche 1) bis 8), dadurch gekennzeichnet, daß der Empfänger (3) eine E-Mail- oder Netzwerkadresse ist.

13. Vorrichtung zur Ausführung des Verfahrens nach einem oder mehreren der Ansprüche 1) bis 8), dadurch gekennzeichnet, daß der Empfänger 3) ein Sprachausgabegerät ist.

5

14. Vorrichtung nach Anspruch 11), dadurch gekennzeichnet, daß das Sprachausgabegerät ein Lautsprecher (34) ist.

15. Vorrichtung nach Anspruch 11), dadurch gekennzeichnet, daß das Sprachausgabegerät ein Telefon (35) ist.

10

16. Vorrichtung zur Ausführung des Verfahrens nach einem oder mehreren der Ansprüche 1) bis 13), dadurch gekennzeichnet, daß der Empfänger (3) eine im Dateneingabegerät (1) eingebauter Funkempfänger ist, welcher die TAN oder das vergleichbare Paßwort auf dem Display oder Monitor des Dateneingabegeräts (1) ausgibt.

15

20

17. Vorrichtung nach Anspruch 14), dadurch gekennzeichnet, daß der Funkempfänger ein Benutzer-Identifizierungselement besitzt.

25

18. Vorrichtung nach Anspruch 15), dadurch gekennzeichnet, daß das Benutzer-Identifizierungselement eine Magnet- oder Chipkarte ist.

19. Vorrichtung nach Anspruch 15), dadurch gekennzeichnet, daß das Benutzer-Identifizierungselement mit grafischen Einrichtungen zur Überprüfung eines Fingerabdruckes oder zu einer Bildidentifizierung des Benutzers arbeitet.

30

35

20. Vorrichtung zur Ausführung des Verfahrens nach einem oder mehreren der Ansprüche 1) bis 17), dadurch gekennzeichnet, daß im Autorisierungsrechner (2) und im Empfänger (3) übereinstimmende Verschlüsselungs-Module vorhanden sind.

40

21. Vorrichtung zur Ausführung des Verfahrens nach einem oder mehreren der Ansprüche 1) bis 18), dadurch gekennzeichnet, daß die Empfangseinheit (4) ein Türschließ-Mechanismus ist.

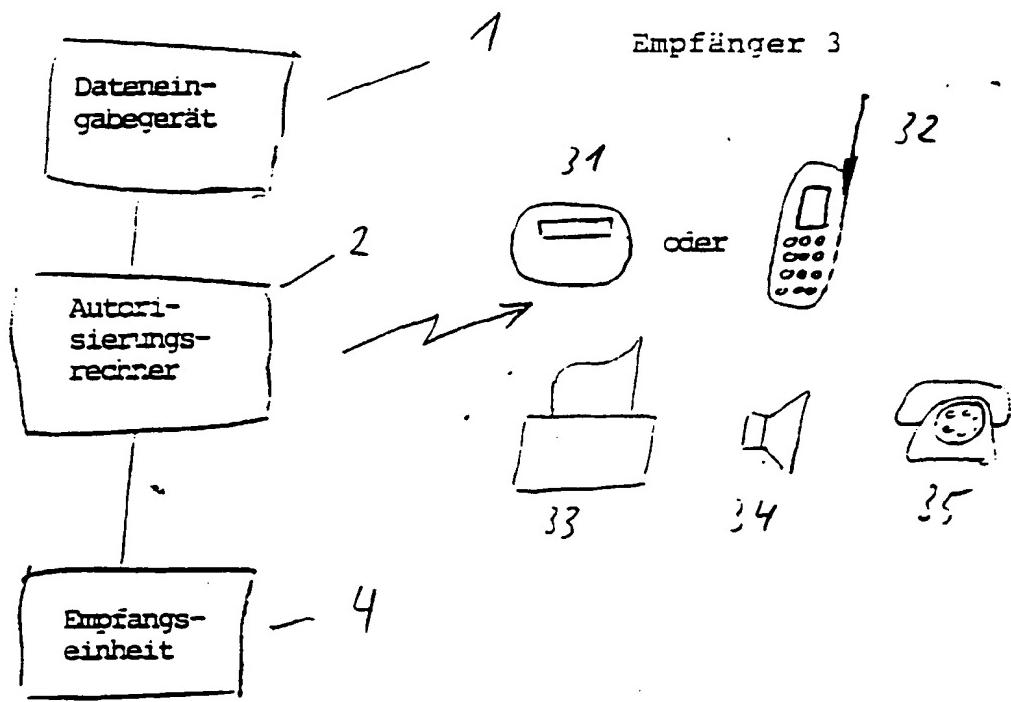
45

22. Vorrichtung zur Ausführung des Verfahrens nach einem oder mehreren der Ansprüche 1) bis 19), dadurch gekennzeichnet, daß der Autorisierungsrechner (2) und die Empfangseinheit (4) in einem Gerät integriert sind.

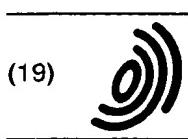
50

23. Vorrichtung zur Ausführung des Verfahrens nach einem oder mehreren der Ansprüche 1) bis 19), dadurch gekennzeichnet, daß das Dateneingabegerät, der Autorisierungsrechner (2) und die Empfangseinheit (4) in einem Gerät integriert sind.

55



THIS PAGE BLANK (USPTO)



(19)

Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 0 875 871 A3

(12)

EUROPÄISCHE PATENTANMELDUNG

(88) Veröffentlichungstag A3:
21.07.1999 Patentblatt 1999/29

(51) Int. Cl.⁶: G07F 19/00, G07F 7/10,
G07C 9/00

(43) Veröffentlichungstag A2:
04.11.1998 Patentblatt 1998/45

(21) Anmeldenummer: 98100688.5

(22) Anmeldetag: 16.01.1998

(84) Benannte Vertragsstaaten:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC
NL PT SE

Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: 29.04.1997 DE 19718103

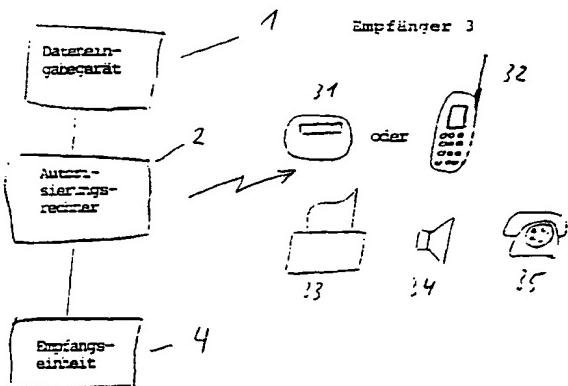
(71) Anmelder: Schmitz, Kim
80539 München (DE)

(72) Erfinder: Schmitz, Kim
80539 München (DE)

(74) Vertreter:
Freiherr von Gravenreuth, Günter, Dipl.-Ing. (FH)
Schwanthalerstrasse 3
80336 München (DE)

(54) Verfahren zur Autorisierung in Datenübertragungssystemen

(57) Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Autorisierung in Datenübertragungssystemen unter Verwendung einer Transaktionsnummer (TAN) oder eines vergleichbaren Paßworts, wobei der Benutzer in einem 1. Schritt über ein Dateneingabegerät seine Identifizierung und/oder eine Identifizierungs-Kennung des Dateneingabegeräts zusammen mit der Aufforderung zur Generierung oder zur Auswahl einer TAN oder ein vergleichbares Paßwort aus einer Datei an einen Autorisierungsrechner sendet, in einem 2. Schritt der Autorisierungsrechner die TAN oder das vergleichbare Paßwort generiert oder aus einer Datei auswählt, in einem 3. Schritt der Autorisierungsrechner die TAN oder das vergleichbares Paßwort über einen anderen Übertragungsweg als in Schritt 1 an einen Empfänger (z. B. Handy oder Pager) sendet, in einem 4. Schritt der Benutzer diese TAN oder das vergleichbare Paßwort von dem Empfänger übernimmt und in das Dateneingabegerät eingibt, in einem 5. Schritt diese TAN oder das vergleichbare Paßwort wieder an den Autorisierungsrechner übermittelt wird, in einem 6. Schritt der Autorisierungsrechner die Gültigkeit der TAN oder des vergleichbaren Paßworts prüft, um dann in einem 7. Schritt einen Verbindungsaufbau zwischen dem Dateneingabegerät und einer Empfangseinheit herzustellen oder freizuschalten.





Europäisches
Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 98 10 0688

EINSCHLÄGIGE DOKUMENTE			
Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betreff Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.6)
X	WO 96 00485 A (ERICSSON TELEFON AB L M) 4. Januar 1996	1, 2, 6-9, 13	G07F19/00 G07F7/10 G07C9/00
A	* das ganze Dokument *	14, 15, 19, 20	

X	WO 95 19593 A (KEW MICHAEL JEREMY :LOVE JAMES SIMON (GB)) 20. Juli 1995	1, 16, 20	
A	* Zusammenfassung *	2, 3, 17	
	* Seite 1. Zeile 3 - Seite 5, Zeile 17 *		
	* Seite 7. Zeile 10 - Seite 11. Zeile 26 *		
	* Abbildungen *		

A	EP 0 416 482 A (HITACHI LTD) 13. März 1991	1, 6, 8-10, 12-20	
	* Spalte 4, Zeile 22 - Spalte 22, Zeile 7		
	*		
	* Abbildungen *		

A	EP 0 745 961 A (AT & T CORP) 4. Dezember 1996		RECHERCHIERTE SACHGEBIETE (Int.Cl.6)

A	US 3 938 091 A (ATALLA MARTIN M ET AL) 10. Februar 1976		G07F

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt			
Recherchenort	Abschlußdatum der Recherche	Prüfer	
DEN HAAG	26. Mai 1999	Bocage, S	
KATEGORIE DER GENANNTEN DOKUMENTE		T : der Erfindung zugrunde liegende Theorien oder Grundsätze E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist D : in der Anmeldung angeführtes Dokument U : aus anderen Gründen angeführtes Dokument S : Mitglied der gleichen Patentfamilie übereinstimmendes Dokument	
<input checked="" type="checkbox"/> von besonderer Bedeutung allein betrachtet <input checked="" type="checkbox"/> von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung erseinen Kategorie <input checked="" type="checkbox"/> technologischer Hintergrund <input checked="" type="checkbox"/> nichtschriftliche Offenbarung <input checked="" type="checkbox"/> Zwischenliteratur			

**ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT
ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR.**

EP 98 10 0688

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.

Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am.
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

25-05-1999

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
WO 9600485	A	04-01-1996	US	5668876 A	16-09-1997
			AU	692881 B	18-06-1998
			AU	2688795 A	19-01-1996
			CA	2193819 A	04-01-1996
			EP	0766902 A	09-04-1997
			FI	965161 A	13-02-1997
			JP	10502195 T	24-02-1998
WO 9519593	A	20-07-1995	AU	1390395 A	01-08-1995
			GB	2300288 A	30-10-1996
EP 0416482	A	13-03-1991	JP	3179863 A	05-08-1991
			DE	69023843 D	11-01-1996
			DE	69023843 T	13-06-1996
			US	5315634 A	24-05-1991
EP 0745961	A	04-12-1996	US	5708422 A	13-01-1998
			CA	2176163 A	01-12-1996
			JP	8339407 A	24-12-1996
US 3938091	A	10-02-1976	KEINE		

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr 12/82

THIS PAGE BLANK (USPTO)